

REMARKS

This paper is being submitted in response to the Office Action mailed in the application on March 29, 2005. Claims 1-30 are pending. Claims 2 and 15 have been cancelled. Claims 1, 3-13, 14 and 16-30 have been amended.

The Examiner has objected to claim 2 because of certain informalities in the claim language. Applicant has cancelled claim 2, thereby rendering the Examiner's objection moot. To the extent that the Examiner has objected to other claims not specifically addressed in the Action by virtue of their dependency or having the same errors in the claim language, applicant submits that all claim dependencies having been changed from cancelled claims 2 and 15 and that no other claims have the same errors in claim language.

The Examiner has rejected applicant's claims 1, 2, 3, 6-16 and 19-30 under 35 U.S.C. § 102(e) as being anticipated by Anderson (U.S. Publication No. 2002/0052923). Although the Examiner has mentioned, on pages 4 and 5, a second reference ("Beck"), the Examiner has not supplied a patent or publication number and has not listed such reference on Form PTO-892 (Notice of References Cited). In view of the above, and because the Examiner has listed grounds for rejection based on "Anderson in view of Beck" under the heading of claim rejections under 35 U.S.C. § 102(e), applicant has treated such rejections to be based on Anderson alone under 35 U.S.C. § 102(e).

The Examiner has rejected applicant's claims 4 and 17 under 35 U.S.C. § 103(a) as being unpatentable over Anderson in view of McArdle et al. (U.S. Patent No. 6,442,686). The Examiner has rejected claims 5 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Anderson in view of Baxter Jr. (U.S. Patent No. 6,385,306). With respect to applicant's claims, as amended, the Examiner's rejections are respectfully traversed.

Applicant's independent claims 1, 13, 14, 26, 27, 28, 29 and 30 have been amended to more clearly recite the feature of the present invention. In particular, claims 1, 14 and 27 are directed to a communication system, a method for controlling a communication system, and a computer executable control program of a communication system, respectively, for providing a Web E-mail service to a client. These claims have been amended to recite means for or steps of managing a key for decrypting an encrypted E-mail, executing authentication of the use allowance of the managed key to the client when the client requests to decrypt the encrypted E-mail, decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated by said authentication means (or in said authentication step), and controlling to transmit the E-mail decrypted by said decrypting means (or in said decrypting step) to the client. Claim 29 has been similarly amended.

Claims 13, 26, 28 and 30 are directed to a communication system, a method for controlling a communication system, a computer executable control program of a communication system, and a storage medium storing a control program of a communication system, respectively, including a client receiving a Web E-mail service from a server. These claims have been amended to recite means for or steps of managing a key for decrypting an encrypted E-mail, executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail, decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated by said authentication means (or in said authentication step), and controlling to transmit the E-mail decrypted by said decrypting means (or in said decrypting step) to said client through a Web. These claims further recite that the client comprises means for or steps of requesting to decrypt the encrypted E-mail, sending the

authentication information to said authentication means (or for authentication in said authentication step), and receiving the decrypted E-mail transmitted by said transmission control means (or in said transmission step).

The present invention teaches a server for providing a Web E-mail service to a client with a management function for managing a secret key and a decrypting function in a public key cryptosystem. The Web E-mail service decrypts the encrypted E-mail and transmits it to an information terminal device, as shown in FIG. 1. The present invention is characterized by a server having management means for managing a key for decrypting an encrypted E-mail, authentication means for authentication of the use allowance of the managed key to the client when the client requests to decrypt the encrypted E-mail, decrypting means for decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated by the authentication means, and transmission control means for controlling to transmit the E-mail decrypted by said decrypting means to the client through a Web. In the present invention, the key for decrypting a message is managed by the server such that the server must authenticate the use allowance of a client of the managed key, and when the allowance is authenticated, the server decrypts an encrypted E-mail and transmits the decrypted E-mail to the client. The client thus does not have to have a key to decrypt the encrypted message. Such construction is neither taught nor suggested by the cited Anderson patent.

More particularly, as shown in FIG. 5, Anderson discloses a process of decrypting a transmitted message in a step S515 and storing the decrypted message in a server in the step S533. The decrypted message to be transmitted is encrypted again in case the decrypted message is retransmitted to the recipient from the server, as described in lines 18-23 of paragraph [0040]. In the process of FIG. 5 of Anderson, there is thus no authentication of the

allowance of the use of a recipient of a managed key of the processing, nor can there therefore be a decrypting of the E-mail upon such authentication and transmission of the decrypted E-mail to the recipient. In Anderson, the E-mail is re-encrypted and the recipient must have a key to decrypt the re-encrypted message.

Accordingly, Anderson does not teach or suggest the features of a server having a management means for executing authentication of the use allowance of the managed key to the client when the client requests to decrypt the encrypted E-mail; authentication means for executing authentication of the use allowance of the managed key to the client; decrypting means for decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated; and transmission control means for controlling to transmit the E-mail decrypted by the decrypting means to the client through the Web, as required by applicant's amended claims.

Applicant's independent claims 1, 13, 14 and 26-30, all of which recite these features, in one form or another, thus patentably distinguish over the Anderson patent. The cited McArdle et al. and Baxter, Jr. patents add nothing to change this conclusion. Applicant's amended independent claims, and their respective dependent claims, are therefore submitted as patentable. Reconsideration of these claims is thus respectfully requested.

If the Examiner believes that an interview would expedite consideration of this Amendment or of the application, a request is made that the Examiner telephone applicant's

counsel at (212) 790-9278.

Dated: June 29, 2005

Respectfully submitted,

*Alexandra B Urban*

COWAN, LIEBOWITZ & LATMAN, P. C.  
1133 Avenue of the Americas  
New York, New York 10036  
T (212) 790-9200

Alexandra B. Urban  
Reg. No. 45,171  
Attorney of Record